

REMARKS/ARGUMENTS

Reconsideration and withdrawal of the rejections of the application are respectfully requested in view of the amendments and remarks herewith, which place the application into condition for allowance. The present amendment is being made to facilitate prosecution of the application.

I. STATUS OF THE CLAIMS AND FORMAL MATTERS

Claims 1-9, 11-20, and 22 are pending in this application. Claims 10 and 21 have been canceled without prejudice or disclaimer of subject matter. Claims 1, 9, 11, 12, 20, and 22, which are independent, are hereby amended. Support for this amendment is provided throughout the Specification, specifically at pages 37, 39, and Figure 10.

No new matter has been introduced. It is submitted that these claims, as originally presented, were in full compliance with the requirements of 35 U.S.C. §112. Changes to claims are not made for the purpose of patentability within the meaning of 35 U.S.C. §101, §102, §103, or §112. Rather, these changes are made simply for clarification and to round out the scope of protection to which Applicants are entitled.

II. REJECTIONS UNDER 35 U.S.C. §103(a)

Claims 1-3, 9, 11-14, 20, and 22 were rejected under 35 U.S.C. §103(a), as allegedly unpatentable over U.S. Patent No. 5,345,508 to Lynn et al. (hereinafter, merely "Lynn") in view of "Concrete Security Analysis of CTR-OFB and CTR-OFB Modes of Operation" to Jaechul et al. (hereinafter, merely "Jaechul").

Claims 4-5 and 15-16 were rejected under 35 U.S.C. §103(a), as allegedly unpatentable over Lynn and Jaechul and further in view of U.S. Patent No. 7,242,772 to Tehranchi et al. (hereinafter, merely "Tehranchi").

Claims 6-8 and 17-19 were rejected under 35 U.S.C. §103(a), as allegedly unpatentable over Lynn, Jaechul, and Tehranchi and further in view of U.S. Patent No. 5,966,450 to Hosford et al. (hereinafter, merely "Hosford").

III. RESPONSE TO REJECTIONS UNDER 35 U.S.C. §103(a)

Claim 1 recites, *inter alia*:

"An encryption apparatus, comprising:

...a path that inputs a part or all the encrypted data that are output from the calculation means to the hold means,

wherein the encryption means reads in parallel the data held by the hold means, one or a plurality of the count values, and a key outputted by the signal generation means, and

wherein the input data is sequentially inputted to the calculation means in a predetermined unit, and the data held by the hold means is reset in each predetermined unit so that data in a preceding unit of the input data is excluded from affecting encryption of a current unit of the input data.
." (emphasis added)

Applicants respectfully submit that Lynn, Jaechul, Tehranchi, and Hosford, taken either alone or in combination, fail to teach or suggest the above-identified features of claim 1. Specifically, nothing is found that discloses or teaches a path that inputs a part or all the encrypted data that are output from the calculation means to the hold means, and wherein the encryption means reads in parallel the data held by the hold means, one or a plurality of the

count values, and a key outputted by the signal generation means, and wherein the input data is sequentially inputted to the calculation means in a predetermined unit, and the data held by the hold means is reset in each predetermined unit so that data in a preceding unit of the input data is excluded from affecting encryption of a current unit of the input data, as recited in claim 1.

Firstly, the path of claim 1 transmits a part or all the encrypted data from the calculation means to the hold means of the encryption apparatus. Applicants submit that the path connects two means in the same encryption apparatus. The path of claim 1, by transmitting encrypted data to the hold means in the same encryption apparatus, allows the encrypted data to be used in the encryption means.

The Final Office Action (see page 4) relies on column 5, lines 12-15 of Lynn to reject the above-identified features of claim 1. Specifically, the Office Action relies on a transmission of cipher text from an encryption device to a receiver to rejection the path of this invention. Applicants respectfully submit that Lynn transmits cipher texts to a receiver, which is not included in the encryption device. Therefore, the transmission of Lynn among separated apparatus does not disclose or suggest the path that within the same encryption apparatus of claim 1.

The Advisory Action dated May 18, 2009 combined Lynn and Jaechul to reject the path cited in claim 1. Specifically, the Advisory Action relies on column 1, lines 21-23 and Figure 1(a) of Lynn to disclose a path between calculation means and hold means and page 109, lines 21-25 of Jaechul to reject using encrypted data in an encryption. Applicants submit that the cited portion of Lynn transmits encrypted data from a transmitter to a receiver through a public

channel. Again, such a transmission is not a transmission of data within the same device or apparatus. Therefore, the rejection based on Lynn is improper.

Secondly, claim 1 recites wherein the encryption means reads in parallel the data held by the hold means, one or a plurality of the count values, and a key outputted by the signal generation means. The encryption means of claim 1 receives in parallel at least three sets of data: a key, counter values, and data of the hold means. In contrast, Lynn's encryption means (see 16 of Figure 2 of Lynn) accepts only two data in parallel: an IV and a Key.

Thirdly, claim 1 recites wherein the input data is sequentially inputted to the calculation means in a predetermined unit, and the data held by the hold means is reset in each predetermined unit so that data in a preceding unit of the input data is excluded from affecting encryption of a current unit of the input data. In contrast, Jaechul's encryption of a current unit takes account into affection of a previous unit, $y_i = f(y_{i-1})$. (see page 109, lines 21-25 of Jaechul)

Therefore, independent claim 1 is patentable.

For reasons similar to, or somewhat similar to, those described above with regard to independent claim 1, claims 9, 11, 12, 20, and 22 are patentable.

IV. DEPENDENT CLAIMS

Each of the other claims in this application is dependent on an independent claim discussed above, and is therefore believed patentable for at least the same reasons presented for the independent claim upon which it depends. Since each dependent claim is also deemed to define an additional aspect of the invention, however, the individual reconsideration of the patentability of each on its own merits is respectfully requested.

Similarly, because Applicants maintain that all claims are allowable for at least the reasons presented hereinabove, in the interests of brevity, this response does not comment on each and every comment made by the Examiner in the Office Action. This should not be taken as acquiescence of the substance of those comments, and Applicants reserve the right to address such comments.

CONCLUSION

In the event the Examiner disagrees with any of statements appearing above with respect to the disclosures in the cited references it is respectfully requested that the Examiner specifically indicate those portions of the reference, or references, providing the basis for a contrary view.

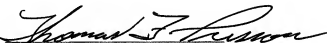
Please charge any additional fees that may be needed, and credit any overpayment, to our Deposit Account No. 50-0320.

In view of the foregoing remarks, it is believed that all of the claims in this application are patentable and Applicants respectfully request early passage to issue of the present application.

Respectfully submitted,

Frommer Lawrence & Haug LLP
Attorneys for Applicants

By:



Thomas F. Presson
Reg. No. 41,442
(212) 588-0800